REMARKS

Claims 1 – 17 are currently pending.

The Office Action dated March 12, 2009 (hereinafter, Office Action) rejects claim 9 pursuant to 35 U.S.C. § 112, second paragraph. Claims 1 – 17 were rejected pursuant to 35 U.S.C. § 103(a) as being unpatentable over Affleck et al. (U.S. Publication No. 2004/0260782) in view of Thompson (U.S. Publication No. 2005/0055709) and in view of Rosner (DE 10121819 A1). Applicant respectfully request reconsideration of these claim rejections in view of the following remarks. Applicant respectfully submits that the claims are in condition for allowance.

I. Claim Rejections – 35 U.S.C. § 112

Claim 9 was rejected pursuant to 35 U.S.C. § 112 because the claim language "is not clear" (Office Action, page 3). The Office Action states that "Claim 9 is indefinite because the claim language "authenticated at the same time" is not clear regarding what exactly constitutes the timing limitation / threshold in terms of interval that is qualified "at the same time" security status" (Office Action, page 3). Applicant respectfully disagrees that claim 9 is unclear. Claim 9 recites checking whether the first authentication and second authentication are authenticated at the same time. Applicant respectfully submits that one skilled in the art would understand the term "at the same time". The first authentication is authenticated at a time that the second authentication is authenticated. Accordingly, Applicant respectfully requests that the claim rejection be withdrawn or further clarified as to what is unclear.

II. Claim Rejections – 35 U.S.C. § 103(a)

Claims 1 – 17 were rejected pursuant to 35 U.S.C. § 103(a) as being unpatentable over Affleck et al. in view of Thompson and in view of Rosner.

Claim 1 recites enabling access authorization to the system technician when the first authentication is authenticated at the first data processing unit and the second authentication is authenticated at the second data processing unit.

Affleck et al. fail to disclose enabling access authorization to the system technician when the first authentication is authenticated at the first data processing unit and the second authentication is authenticated at the second data processing unit. The Office Action confirms that "Affleck as modified does not disclose expressly enabling access authorization to the system technician when the first authentication is authenticated at the first data processing unit and the second authentication is authenticated at the second data processing unit" (Office Action, page 6, emphasis removed). Instead, the Office Action relies on Rosner.

Rosner fails to disclose enabling access authorization to the system technician when the first authentication is authenticated at the first data processing unit and the second authentication is authenticated at the second data processing unit. The Office Action cites the Abstract as disclosing this feature. Applicant respectfully disagrees. The cited Abstract sets forth a "[m]ethod for controlling access to electronically stored data in distributed heterogeneous environments in which data access is only granted when two or more persons are present to authorize the access" (Abstract, lines 1 – 5). Furthermore, the Abstract provides an example where "both a patient and a doctor must be present with their own access chip card [before] medical records can be accessed" (Abstract, lines 11 – 13). In other words, the patient and doctor are about to view a patient's record. The patient and doctor sit down at the same machine and provide their own access chip cards. The patient records can not be accessed without both access cards. Rosner discloses a single machine (See, e.g., Figure 1). Rosner does not disclose that the patient is at a first data processing unit and the doctor is at a second data processing unit. Accordingly, Rosner does not disclose enabling access authorization to the system technician when the first authentication is authenticated at a first data processing unit and the second authentication is authenticated at a second data processing unit. Therefore, claim 1 is allowable over the cited references.

Furthermore, claim 1 is also allowable over the cited references for additional reasons that are independent of those discussed above and should be considered independently of the remarks set forth above. Claim 1 is allowable because one skilled in the art at the time of the the application was filed would not have combined the cited portions of Affleck et al. and Rosner. Affleck et al. disclose a "security module 550 [that] allows the system administrator to edit access rights of each of the technicians" (¶ [060]; emphasis added). Rosner states that the "invention relates to accessing patient records" (Abstract). In other words, Rosner is directed to allowing a doctor and patient view the patient records. One skilled in the art would not combine Affleck et al. and Rosner because they are directed to two materially different technologies. Affleck et al. is directed to providing access rights (i.e., system administrator and technician). Rosner is directed to viewing patient records (i.e., doctor and patient). Therefore, claim 1 is allowable over the cited references for at least this reason.

Finally, claim 1 is allowable over the cited references for yet additional reasons that are independent of those discussed above and should be considered independently of those remarks set forth above. Claim 1 is allowable because the cited references fail to disclose authenticating the system administrator on a first data processing unit by transferring the first authentication to an authentication program, as recited in claim 1. The Office Action cites Affleck et al. as disclosing this feature.

Affleck et al. fail to disclose authenticating the system administrator on a first data processing unit by transferring the first authentication to an authentication program. The Office Action cites the security module 550 as disclosing this feature. The security module 550 is an element of the system administration module 410 (¶ [065]). The Office Action states that ¶ [066] discloses that "the security module within the ADMIN module allows an authenticated system administrator to edit access rights for each of the system technicians" (Office Action, page 3). However, ¶ [066] does not disclose "an authenticated system administrator." Instead, Affleck et al. states that "[t]he security module 550 allows the system administrator to edit access rights of each of the technicians. Access rights for individual technicians, or groups of technicians, may be set or edited, and logon attempts may be monitored" (¶ [066]). There is no mention that the system administrator is

authenticated. Even under the interpretation that the system administrator is authenticated, Affleck et al. is completely silent as to transferring the first authentication to an authentication program. Therefore, claim 1 is allowable over the cited references.

Neither Affleck et al, Thompson, nor Rosner, either alone or in combination, disclose enabling access authorization to the system technician when the first authentication is authenticated at the first data processing unit and the second authentication is authenticated at the second data processing unit, the first data processing unit being remote from the second data processing unit, as recited in claim 5. The cited references also fail to disclose checking whether the first authentication and second authentication are authenticated at the same time; and enabling access authorization to the system technician when the first authentication and second authentication are authenticated at the same time, as recited in claim 9. Accordingly, claims 5 and 9 are allowable over the cited references.

Dependent claims 6-8 and 10 – 17 depend from allowable claims 5 and 9 and are allowable for at least these reasons. As discussed below, further limitations of the dependent claims may be allowable over the cited references.

Claim 10 recites that the data processing system processes data that can be accessed by individuals with a simple authorization according to the two man principle when the particular authorization is not present. The cited references fail to disclose the two man principle. The two man principle may be defined as follows:

> **two-person integrity** A security practice designed to prevent an individual from having solitary access to sensitive data, equipment or other material. Two-person integriaty requires at least two authorized individuals to be involved in the performance of a task, each capable of detecting incorrect or unauthorized security probedures with respect to the task being performed. On person performs the task and the other keeps a watchful eye on its be being performed. *See*, Newton's Telecom Dictionary, Copyright © Harry Newton, 24th Edition

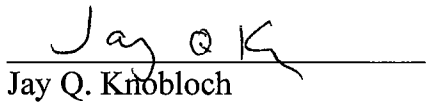
One skilled in the art would understand that the cited portion of Affleck et al. does not disclose the two-man principle. Therefore, claim 10 is allowable over the cited references.

Conclusion

For at least the reasons presented above, the Applicant respectfully submits that the pending claims are in condition for allowance.

The Examiner is respectfully requested to contact the undersigned in the event that a telephone interview would expedite consideration of the application.

Respectfully submitted,



Jay Q. Knobloch
Registration No. 57,347
Agent for Applicants

BRINKS HOFER GILSON & LIONE
P.O. BOX 10395
CHICAGO, ILLINOIS 60610
(312) 321-4200